UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/419,828	10/14/1999	DON VAN DYKE	M-7084-US	1859

23418 7590 06/07/2004

VEDDER PRICE KAUFMAN & KAMMHOLZ
222 N. LASALLE STREET
CHICAGO, IL 60601

EXAMINER	
SMITHERS, MATTHEW	

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 06/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/419,828	DYKE ET AL.	
	Examiner	Art Unit	
	Matthew B Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-13 and 15-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-13 and 15-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1, 3-13, and 15-21 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent 6,088,800 granted to Jones et al.

Regarding claim 1, Jones meets the claimed limitations as follows:

"A computer system capable of performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

an arithmetic logic unit having a logic circuit for performing expansion permutation, S-box substitution, P-box permutation and associated XOR operations

wherein said computer system further comprises a register file providing operands to said arithmetic logic unit; and

wherein said register file includes general purpose registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 3, Jones meets the claimed limitations as follows:

"The method of claim 1, wherein said register file includes a first register for storing a first portion of a datum for said encryption or decryption, a second register for storing a

second portion of said datum and a third register for storing a subkey." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 4, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said datum is 64 bits long and said subkey is 48 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 5, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first and second portions each contain one-half number of bits of said datum." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 6, Jones meets the claimed limitations as follows: "The computer system of Claim 5, wherein each of said first and second portions is 32 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 7, Jones meets the claimed limitations as follows: "The computer system of Claim 3, wherein said first, second and third registers store operands of an instruction executing one round of said DES algorithm using said logic circuit and a shift circuit in said arithmetic logic unit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said

instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 8, Jones meets the claimed limitations as follows: "The computer system, of Claim 7, wherein a bypass mechanism is provided in said register file such that said results are provided as input to said logic circuit without first being written back to said first, second and third registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 9, Jones meets the claimed limitations as follows: "The computer system of Claim 8, wherein said register file and said bypass mechanism are shared by all instructions in said arithmetic logic unit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 10, Jones meets the claimed limitations as follows: "The computer system of Claim 1, further comprising a second logic circuit capable of performing key selection for said DES algorithm, said second logic circuit operating in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 11, Jones meets the claimed limitations as follows: "The computer system of Claim 1, wherein said logic circuit further comprises a circuit for selecting a subkey from a key." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 12, Jones meets the claimed limitations as follows:

"The computer system of Claim 11, wherein said key is 56 bits long." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 13, Jones meets the claimed limitations as follows:

"A process for performing encryption or decryption under a Data Encryption Standard (DES) algorithm, comprising:

providing a logic circuit in an arithmetic logic unit; and performing expansion permutation, S-box substitution and P-box permutation and associated XOR operations in said logic circuit; and

storing operands in a register file; and providing said operands to said logic circuit;

wherein said register file includes general purpose registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 15, Jones meets the claimed limitations as follows:

"The process of Claim 13, further comprising: storing operands in a register file; and providing said operands to said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 16, Jones meets the claimed limitations as follows:

"The process of Claim 15, further comprising: storing a first portion of a datum for said encryption or decryption in first register in said register file; storing a second portion of

said datum for said encryption or decryption in second register in said register file; and storing a subkey for said encryption or decryption in third register in said register file." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 17, Jones meets the claimed limitations as follows: "The process of Claim 16, further comprising storing operands of an instruction executing one round of said DES algorithm in said first, second and third registers using said logic circuit and said shift circuit, said instruction designating to store results in said first, second and third registers in such manner as to allow said results in said first, second and third registers to be operands in a subsequent execution of said instruction." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 18, Jones meets the claimed limitations as follows: "The process of Claim 17, further comprising providing said results as input to said logic circuit without first being written back to said first, second and third registers." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 19, Jones meets the claimed limitations as follows: "The process of Claim 13, further comprising selecting a subkey from a key for said DES algorithm in a second logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 20, Jones meets the claimed limitations as follows:

"The process of Claim 19, further comprising operating said second logic circuit in parallel with said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Regarding claim 21, Jones meets the claimed limitations as follows:

"The process of Claim 13, further comprising selecting a subkey from a key using a key select circuit in said logic circuit." see column 6, lines 3-13; column 7, lines 15-38; column 16, line 57 to column 18, line 13 and figures 2, 4, 5, 6, and 14.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-13, and 15-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. patent 6,266,418 granted to Carter et al and further in view of U.S. patent 5,958,038 granted to Agrawal et al.

Regarding claims 1 and 13, Carter teaches a computer system performing encryption under a DES algorithm using logical operators (see column 5, lines 51-61 and column 8, lines 6-18). However Carter fails to specifically teach the computer system has an arithmetic logic unit (ALU) and a register file with general purpose registers (GPR's). Agrawal teaches a computer system for performing encoding of data streams using an ALU and register files with GPR's (see column 6, lines 35-51). It

would have been obvious to one of ordinary skill in the art at the time of the invention to combine Carter's apparatus for encrypting communications with Agrawal's method of encoding streamed data in order to gain the advantage of producing a faster stream of encoded (encrypted) data between the communication devices (see Agrawal; column 2, lines 15-24).

Regarding claims 3-12 and 15-21, Carter as modified teaches performing encryption on a 64-bit datum and using a 56-bit traffic key (see Carter; column 5, lines 51-61 and column 8, lines 6-18).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew B Smithers
Primary Examiner
Art Unit 2137